PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04N 1/44, 7/167 — A1

(11) International Publication Number: WO 00/31964

(43) International Publication Date: 2 June 2000 (02.06.00)

(21) International Application Number: PCT/SE99/02106

(22) International Filing Date: 17 November 1999 (17.11.99)

(30) Priority Data: 9803979-5, 20 November 1998 (20.11.98), SE

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors: JÄNDEL, Magnus; Vårvägen 10, S-194 60 Upplands Väsby (SE). LARSSON, Mathias; Laxgatan 17, 5 tr, S-133 43 Saltsjöbaden (SE).

(74) Agents: SANDSTRÖM, Staffan et al.; Bergenstråhle & Lindvall AB, Box 17704, S-118 93 Stockholm (SE).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

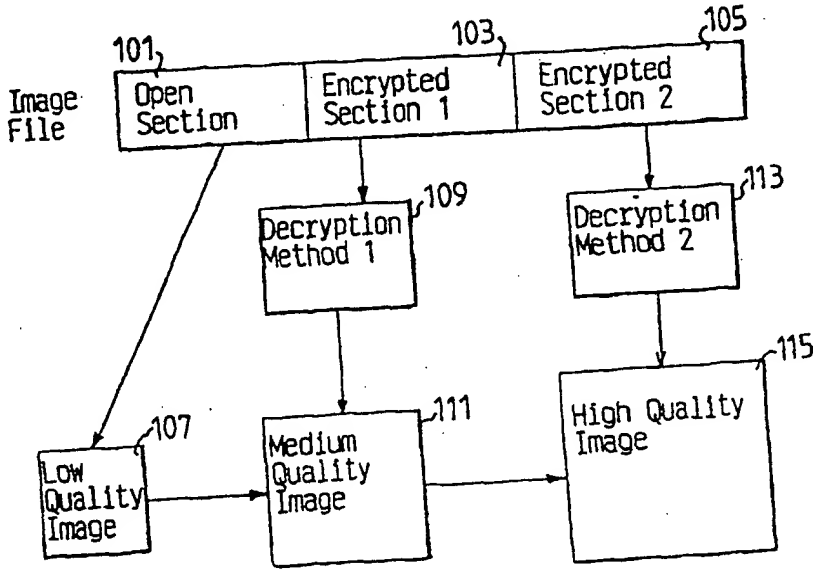
With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: A METHOD AND A DEVICE FOR ENCRYPTION OF IMAGES

(57) Abstract

In a method and a device for partial encryption and progressive transmission of images, a first section of the image file is compressed at reduced quality without decryption, and a second section of the image file is encrypted. Users having access to appropriate decryption keywords can decrypt this second section. The first section together with the decrypted second section can then be viewed as a full quality image. The storage space required for storing the first and section together is essentially the same as the storage space required for storing the unencrypted full quality image. By using the method and device as described herein storage and bandwidth requirements for partially encrypted images is reduced. Furthermore, object based composition and processing of encrypted objects are facilitated, and ROIs can be encrypted. Also, the shape of a ROI can be encrypted and the original object can be decrypted and restored in the compressed domain.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

A METHOD AND A DEVICE FOR ENCRYPTION OF IMAGES

TECHNICAL FIELD

The present invention relates to a method and a device for encrypting images.

BACKGROUND OF THE INVENTION AND PRIOR ART

Encryption of digital data is a technical field which becomes important when transmitting and storing secret information or information which only shall be available to a user paying for the information. Thus, several methods for encrypting digital data are in frequent use. Such methods can also be applied also to digital image data. Examples of encryption methods are DES, triple DES and the public-key RSA method.

Digital images can be stored on servers and distributed over a telecommunication network as digital image data. Images can also be distributed using a physical storage medium such as a CD-ROM. Service providers need to establish access control that suits their business model. In this context it might be suitable to offer partial access to one set of users and full access to another set of users. Thus, some of the image data must be encrypted in order to prevent all users from having full access to all image data.

News photographs can e.g. be offered for sale on the Internet. The service provider wants to allow customers to download a version of the image with reduced quality for evaluation. Journals, that want to publish an image, pay for the service and are then allowed to download a full quality image.

However, such a service provider wants to minimize storage space and download bit rates. An image provider might alternatively want to distribute images on e.g. a CD-ROM. CD-ROMs are given away or sold for a low price. Customers can view the images at a reduced quality, but they must pay for viewing them at full quality. In the case the image provider wants to use the storage space on the CD-ROM as efficiently as possible.

A reduced quality image can be produced according to several different main schemes, such as:

1) Reduced resolution
2) Reduced accuracy of the transform coefficients.
3) Exclusion of predefined regions of interest (ROI)

These methods can be combined so that a reduced quality image is e.g. produced by reducing both the resolution and the accuracy of the transform coefficients.

By using the method and device for storing and transmitting image data as described herein, several advantages are obtained. Thus, there is no need to store two different versions of an image if different users are to have access to different quality of the one and same image. Also, transmission times become much lower if the information content of the first, low resolution, image data can be reused when transmitting the higher resolution image data.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described in more detail and with reference to the accompanying drawings, in which:

- Fig. 1 is a general view of the file structure of an image.
- Figs. 2a and 2b shows encryption of images coded according to the JPEG 2000 standard.
- Fig. 3 is a flow chart illustrating some steps carried out when encrypting an image.
- Fig. 4 is a diagram illustrating a client server process.
- Fig. 5 is a view of an encryption header

DETAILED DESCRIPTION

In Fig. 1, a general view of the file structure of an original, high resolution, image is shown. Thus, the image data file consists of a number of different independently decodable coding sections 101, 103 and 105. In the file structure shown in Fig. 1, the section 101, which is a low resolution version of a high resolution image, is coded without encryption and will therefore be possible to decode by any receiver.

The section 103, which comprises data, which combined with the data of section 101, result in a medium resolution version of the high resolution image, is encrypted using a first encryption method, and only receivers having access to the correct encryption key will be able to decode the data stored in the section 103.

The section 105, which comprises data, which combined with the data of section 101 and 103 results in a full resolution version of the high resolution image, is encrypted using a second encryption method, and only receivers having access to the encryption key will be able to decode the data stored in the section 105.

Thus, decoding of the section 101 will result in a low resolution image version 107. Decryption 109 and decoding of the section 103 will, combined with the image data from the section 101 result in a medium resolution image 111. Decryption 113 and decoding of the section 105 will, combined with the image data from the sections 101 and 103 result in a full resolution image 115.

Furthermore, implementation in the JPEG 2000 standard without ROI, see Charilaos Christopoulos (ed.) JPEG 2000 Verification Model Version 2.0, describes how each coding unit of the JPEG 2000 bitstream can be inserted in the bitstream so that a wide range of progressive modes can be supported.

In JPEG 2000 verification model 2.0, a coding unit is a part of the bitstream that encodes a specific bitplane of a given subband. In general, a coding unit can be described as any independently decodable subset of image information. The general mechanism for specifying the bitstream order is to include so called tags that specifies the next coding unit (it is sufficient to specify the subband since the bitplane order is known). Several specific modes can be defined in the header that defines a default coding unit order thus saving the bits that are needed for inserting explicit tags.

In Figs. 2a and 2b block diagrams describing how encryption can be implemented in the JPEG 2000 encoder and decoder respectively, are shown.

Thus, in Fig 2a a block diagram where encryption is performed after entropy coding in the encoder is shown. Coding units enter an entropy coding block 201. In the block 201 coding the coding units are entropy coded using some suitable entropy code. The output from the block 201 is fed to a selector which selects a suitable encryption method for each entropy coded coding unit. Some coding units can be selected to not be encrypted at all.

In response to the selection made in the selector 203 the entropy coded coding units are encrypted in a block 205. The encrypted coding units together with the not encrypted coding units then form a combined output data stream, which can be stored or transmitted.

In Fig. 2b a decoder for decoding the bit stream generated by the encoder in Fig. 2a is shown. Thus, first encrypted and not encrypted coding units enter the decoder via a selector 251, which selects a suitable decryption method for each entropy coded coding unit, or if the received coding unit is not encrypted it is directly transmitted to a block 255.

In response to the selection made in the selector 255 the entropy coded coding units are decrypted in a block 253 using a suitable decryption algorithm. The decrypted coding units are then fed to the block 255. In the block 255 the coding units from fed directly from the selector 251 and from the decryption block 253 are entropy decoded and combined to form a combined output data stream corresponding to the data stream which is fed to the entropy coding block 201 in Fig. 2a.

Each coding unit in the transmission scheme as shown in the Figs. 2a and 2b is handled as an independently encrypted block. Each coding unit can also be encrypted separately with any user supplied encryption method. Different units in the same image can be encrypted with different encryption methods. The

encryption method used can further be an encryption algorithm combined with a keyword or a method for generating keywords.

Different encryption methods can in such an embodiment have identical algorithms but different keywords. Encryption Method Description (EMD) as shown in Figs. 2a and 2b is any global data such as session keywords or algorithm identifiers that is needed to specify the Encryption Method. Unit Encryption State (UES) is a symbol that for each coding unit defines how it is encrypted.

In Fig. 3, a flow chart illustrating different steps carried out when encrypting an image are shown. First, in a step 301, an image to be partially encrypted is received. The image received in step 301 is then coded using a coding algorithm generating independently decodable coding units, e.g. JPEG 2000, in a step 303.

Next, in a step 305, some of the coding units of the image coded in step 303 are encrypted using some suitable encryption method, such as DES. The coding units that are chosen to be encrypted can be set in accordance with user preferences. Thus, a user can chose to have coding units corresponding to ROIs, higher order bit-planes, etc, encrypted. Finally, the encrypted coding units and the coding units which are not encrypted are merged into a single bit stream.

In Fig. 4, a flow chart illustrating a client-server process, when transmitting an image encoded according to the method as described in conjunction with Fig. 3 is shown. Thus, a client 401 is connected to a server 403. The client 401 can then issue a request towards the server 403 for a particular image, step 405.

The server 403 replies by transmitting the coding units of the image which are not encrypted, step 407. The not encrypted coding units can be decoded by the client who now will have access to a low resolution version or a part of the full image. Based on this information the client may wish to have access to the image in a higher resolution or the full image. If so the

client transmits a request to the server requesting such information, step 409.

The server replies by sending a request to the client requesting the client to agree to the conditions for transmitting the higher resolution version of the image, step 411. If the client agrees via a message 413, e.g. comprising a card number or account number from which to bill the cost for the image, the server sends the encrypted coding units together with a key word by means of which the encrypted coding units can be decrypted, step 415. A secure method for key distribution should be used. Examples of such secure methods are described in W. Stallings "Data and computer Communications", p 635 -637, Prentice-Hall 1997 fifth edition ISBN 0-13-571274-2.

If the client already has access to the unencrypted and encrypted coding units, for example if he has purchased a CD-ROM with images coded as described herein. The scheme as described in conjunction can be modified so that no image data is transmitted. Instead the client only agrees to conditions set by the server in order to have access to the key word(s) which are required to decrypt the encrypted coding units of the CD-ROM.

In the case when the method and device as described herein is used when encoding image according to the JPEG 2000 standard, it is advantageous if the JPEG 2000 standard does not standardise encryption methods. An Encryption Header that is included in the image header or optionally an Encryption Tag that is merged with the JPEG 2000 Tags can instead be used to specify how coding units are decrypted.

In such an embodiment the JPEG 2000 image header contains an Encryption Flag (EF). EF is then set if any coding unit is encrypted. An Encryption Header (EH) should then be appended to the JPEG 2000 image header and encryption information can optionally be merged into JPEG 2000 Tags.

In Fig. 5 an encryption header is shown. The Encryption Header can in such an embodiment contain the following symbols.

1) Encryption Mode (EM). A set of standard encryption modes are defined e.g.

a) One encryption method is used for all coding units
b) Bitplanes of less significance than bitplane X are encrypted
c) Subbands of higher resolution than Y are encrypted
d) ROIs specified in are encrypted, etc.

No encryption information need to included in the Tags if an EM is defined.

2) Encryption Mode Parameters (EMP). Parameters (X, Y, ...) that are used to define the Encryption Mode are set here.

3) Number of encryption methods used. Several encryption methods can be used within the same image if e.g. different user groups should be allowed to see different image content.

4) One Encryption Method Descriptor (EMD) for each encryption method. The EMD defines any data that is needed by the encryption/decryption module. The type of encryption algorithm is defined. A typical use of EMD will be to include a keyword that is encrypted by a public key algorithm. The user supplies a private key for decrypting the enclosed encrypted key. The decrypted key is used by a fast decryption algorithm to decrypt image coding units. The order of the EMDs allocates an number to each encryption method. This number is used in UES symbols.

5) The bitstream must for each coding unit specify if it is encrypted and if so by what method. This is done by setting one Unit Encryption State (UES) symbol per coding unit. These symbols could either be collected in the encryption header or alternatively be distributed in the bitstream as encryption tags. If the UES information is kept in the encryption header we define a header element - Encryption State (ES). ES consists of a series of UES symbols that are listed in the same order as the coding units appears in the bit stream.

IF EF is set and the Encryption State is not given in the

header, JPEG 2000 Tags can be expanded to contain Unit Encryption State (UES) symbols. UES defines which encryption method, if any, that is used for encrypting the next coding unit.

The transform coefficients belonging to a ROI can be handled as described above. They can be completely or partially encrypted by selecting appropriate coding units belonging to the ROI for encryption.

The main problem is that the shape of the ROI might reveal the content. If the shapes are encrypted it is, however, difficult to show a reduced quality image since it is difficult to interpret the coded transform coefficients.

This problem can be solved by defining a so called cloaking shape (c-shape). Thus, the real shape of one or several ROIs are completely enclosed in the c-shape. The c-shape is designed to not reveal sensitive image content. A simple example of a c-shape is a bounding box.

A c-shape is treated as one single ROI in the JPEG 2000 bit stream. The c-shape is coded without encryption as described in Charilaos Christopoulos (ed.), JPEG 2000 Verification Model Version 2.0. According to the technique as described therein this would result in that the shape is defined in the JPEG 2000 header.

A mask is created using the c-shape and the transform coefficients belonging to the c-shape is coded and encrypted using the method as described herein. This will result in that all coefficients belonging to any of the ROIs that are shielded by the c-shape are encrypted. The texture of the ROIs is thus protected by encryption.

The shape of the ROIs are encrypted and stored e.g. in the encryption header. The encryption header contains pointers that links encrypted ROI shapes with the corresponding c-shape. The decoder can now decode the unencrypted background. The c-

shape can be displayed as a blank region. The original ROIs can be decoded if the keyword is known. This is done by decrypting the coefficients belonging to the c-shape. The shape of each ROI belonging to the c-shape is also decrypted. The bitstream can now be rearranged so that the c-shape is dropped and the original ROI data structures are restored. Note that this is done in the compressed domain.

The mask that is used for encoding a ROI is not uniquely defined in JPEG 2000. A mask that is sufficiently large so that the ROI is encoded lossless will often cover the whole lower subbands. A mask that is not allowed to expand will lead to a lossy encoding of the ROI. The masks belonging to different ROIs or to a ROI and the background can be designed to overlap. This means that some coefficients are encoded in more than one ROI. Such overlap will lead to a reduced overall compression but the ROIs are more independent so that any ROI can be accessed and decoded with a good visual result.

The partial encryption method for ROIs described herein is not dependent of the choice of mask as long as the mask is selected so that the content of a ROI cannot be reconstructed from the content of any other ROI or background. A method for building a mask that hides the content of the ROI is described in Charilaos Christopoulos (ed.), JPEG 2000 Verification Model Version 2.0.

By using the method and device as described herein storage and bandwidth requirements for partially encrypted images is reduced. Furthermore, object based composition and processing of encrypted objects are facilitated, and ROIs can be encrypted. Also, the shape of a ROI can be encrypted and the original object can be decrypted and restored in the compressed domain.

Another advantage is that encryption does not need to be performed at the same time as encoding the image. Thus, since the process takes place in the compressed domain (at the bitstream syntax) it is possible to encode all images without encryption. The encryption can be performed just before transmitting the image by a parser (transcoder). In this case,

if the encryption increases the bitrate, which will be the case if the encryption is placed in the TAGS, the increase in bitrate is avoided and the encryption information is only added before transmitting it.

CLAIMS

1. A method of partially encrypting image data comprising the steps of:
- coding the image data using an encoding algorithm generating independently decodable coding units,
- encrypting at least one of the coding units, and
- merging coding units which are not encrypted with coding units which are encrypted into a combined bitstream.

2. A method according to claim 1, **characterized** in that the not encrypted coding units correspond to a low resolution version of the image data.

3. A method according to any of claims 1 - 2, **characterized in** that different coding units are encrypted using different coding methods.

4. A method according to any of claims 1 - 3, **characterized in** that an encryption flag, which indicates if a coding unit is encrypted, is inserted in the bit stream.

5. A method according to any of claims 1 - 4, when information corresponding to a Region of interest is encrypted, **characterized** in that the shape of the region of interest is enclosed in a cloaking shape.

6. A device for partial encryption of image data **characterized by:**
- means for coding the image data according to an encoding algorithm generating independently decodable coding units,
- means connected to the coding means for encrypting at least one of the coding units, and
- means for merging coding units which are not encrypted with coding units which are encrypted as a combined bitstream.

7. A device according to claim 6, **characterized by** means for selecting the not encrypted coding units as units corresponding to a low resolution version of the image data.

8. A device according to any of claims 6 - 7, **characterized by** means for encrypting different coding units using different coding methods.

9. A device according to any of claims 6 - 8, **characterized by** means for inserting an encryption flag, which indicates if a coding unit is encrypted, in the bit stream.

10. A device according to any of claims 6 - 9, **characterized by** means for enclosing a region of interest shape in a cloaking shape.

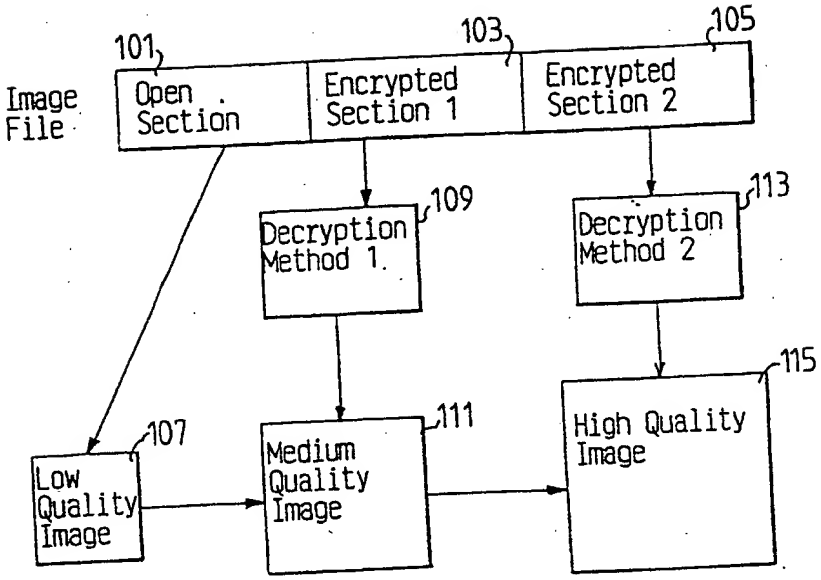


FIG.1

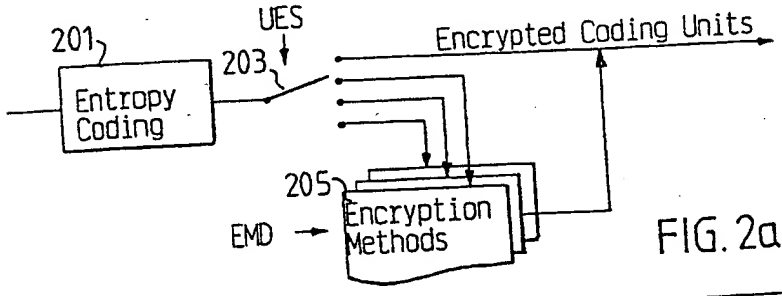


FIG. 2a

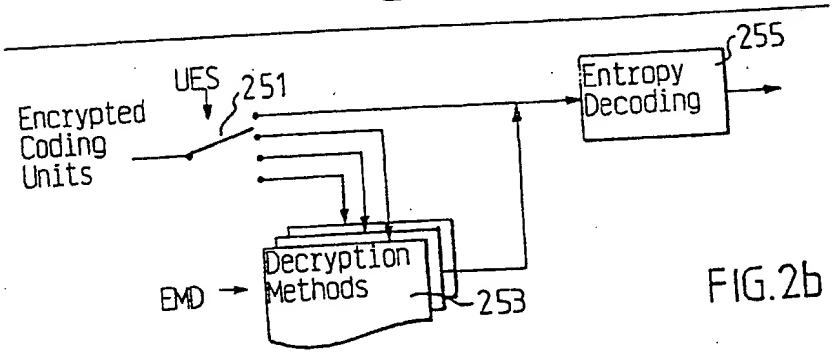


FIG.2b

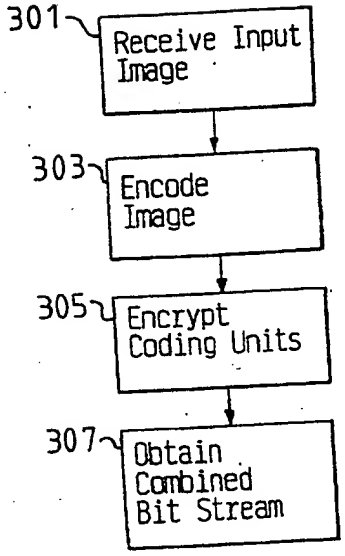

301
Receive Input Image
303
Encode Image
305
Encrypt Coding Units
307
Obtain Combined Bit Stream

FIG. 3

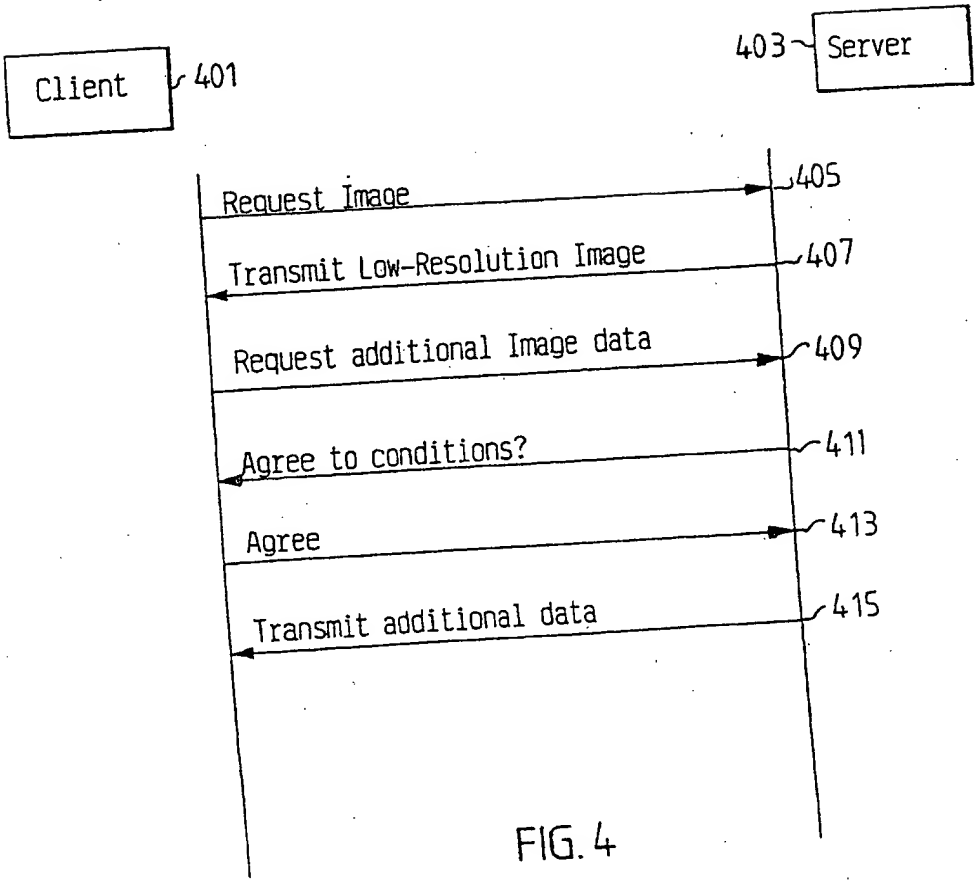

Client
401
403
Server
Request Image
405
Transmit Low-Resolution Image
407
Request additional Image data
409
Agree to conditions?
411
Agree
413
Transmit additional data
415

FIG. 4

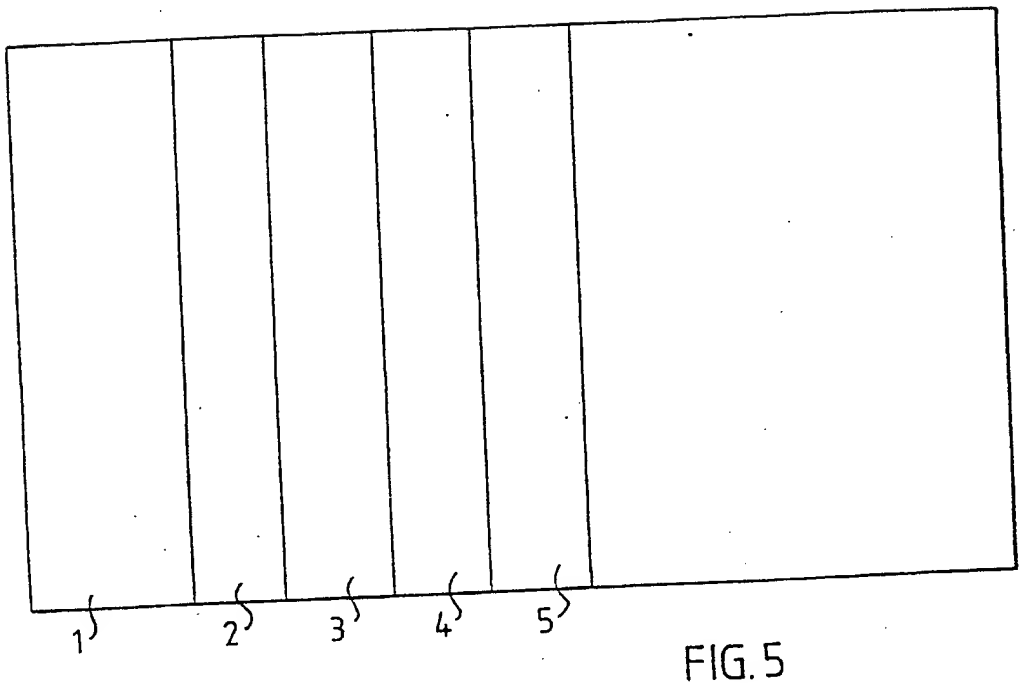


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 99/02106

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04N 1/44, H04N 7/167
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0614308 A1 (EASTMAN KODAK COMPANY), 7 Sept 1994 (07.09.94), claims 1,5, abstract --	1-10
A	EP 0649261 A2 (CANON KABUSHIKI KAISHA), 19 April 1995 (19.04.95), claims 1-28 --	1-10
A	NL 1005523 C (TECHNISCHE UNIVERSITEIT EINDHOVEN TE EINDHOVEN), 2 November 1998 (02.11.98), figure 1 --	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" erlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 March 2000	31 -03- 2000
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson/AE Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

Information on patent family members

02/12/99

International application No.
PCT/SE 99/02106

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0614308 A1	07/09/94	JP 6301754 A	28/10/94
EP 0649261 A2	19/04/95	JP 7115638 A	02/05/95
		US 5933499 A	03/08/99
NL 1005523 C	02/11/98	NONE	